University Health Network
Policy & Procedure Manual
Administrative: Privacy

Policy

University Health Network (UHN) maintains privacy in compliance with the Personal Health Information Protection Act (PHIPA) 2004, as well as taking into account the Personal Information Protection and Electronic Documents Act (PIPEDA). PHIPA establishes rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care. PIPEDA sets ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

To protect patient privacy and ensure the proper use of personal health information, UHN agents must adhere to UHN privacy policies and standards.

As a health information custodian, UHN and its agents (including employees, physicians, contractors, consultants, volunteers, students and other workers at UHN, including all personnel affiliated with third-parties) are responsible for ensuring that the personal health information of our patients is treated with respect and sensitivity.

UHN will follow the standards set by PHIPA in:

- The collection, use, and disclosure of personal health information (PHI).
- Providing individuals with a right of access to PHI about themselves, subject to limited and specific exceptions set out in PHIPA.
- Providing individuals with a right to require the correction or amendment of PHI about themselves, subject to limited and specific exceptions set out in PHIPA.
- Providing for independent review and resolution of complaints with respect to PHI.
- Providing effective remedies for contraventions of PHIPA.
- Providing guidance material pertaining to privacy standards.

Consent for the Collection, Use & Disclosure of Personal Health Information

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal health information, except where inappropriate. (Refer to Consent for the Collection, Use & Disclosure of Personal Health Information on the Privacy website.)

In certain circumstances, PHI can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. Seeking consent may be impossible or inappropriate, for example when the individual is seriously ill or mentally incapacitated. In these circumstances, consent of the individual's substitute decision maker will be sought, where feasible.

UHN may use or disclose personal health information for research purposes without an individual's consent if strict conditions are met (e.g. the approval of a Research Ethics Board), as per PHIPA. For example, a custodian who uses PHI for research and, similarly, a researcher who seeks disclosure of personal health information for research, must both submit a detailed research plan to the UHN Research Ethics Board (REB) for approval. In reviewing a research proposal involving the use and disclosure of personal health records, the REB must consider:

- whether the research cannot be reasonably accomplished without access to the information
- the public interest in conducting the research and in protecting privacy
- whether obtaining consent directly is impracticable
- whether adequate safeguards are in place to protect the privacy of individuals and the confidentiality of their information

Limiting the Collection, Use & Disclosure of Personal Health Information

The collection of PHI will be limited to that which is necessary for the purposes identified by UHN; information will be collected by fair and lawful means.

At or before the time PHI is collected, UHN will identify the purposes for which the personal health information is collected. Permitted purposes include:

- the delivery of direct patient care
- the administration of the health care system
- research
- teaching
- statistics
- fundraising
- meeting legal and regulatory requirements as described in PHIPA

UHN may use information from non-UHN organizations if UHN has authority to use for the direct care of a patient.

Refer to Limiting Collection, Use and Disclosure of Personal Health Information on the Privacy website.

Retention, Archiving & Destruction of Personal Health Information

UHN has established information retention guidelines that define consistent minimum standards and requirements for the length of time PHI and records of personal health information are to be maintained. (Refer to Access to Archival Records policy 1.30.008).

UHN has established appropriate practices for the timely and secure disposal of PHI consistent with confidentiality, legal and regulatory requirements. (Refer to Storage, Transport & Destruction of Confidential Information policy 1.40.006).

Researchers are responsible for the storage/retention of research data, as defined in their approved research protocol.

Patients' Rights

Upon request, an individual will be informed of the existence, use, and disclosure of his or her PHI, and will be given access to that information as per Patient Access to the Medical Record policy 1.40.003 and Release of Patient Information policy 1.40.002. UHN agents may not access their own paper and/or electronic records outside of this process and, by extension, may not directly view their own records in electronic systems.

UHN will make specific information about its policies and practices relating to the management of PHI readily available to individuals. (See Patient Access to the Medical Record policy 1.40.003.)

An individual will be able to address a challenge concerning compliance with this policy.

UHN will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.

UHN will investigate all complaints. If a complaint is found to be justified, UHN will take appropriate measures, including amending its policies and practices if necessary.

Ensuring Accuracy of Personal Health Information

UHN will take reasonable steps to ensure that information is as accurate, complete, and relevant as is necessary to minimize the possibility that inappropriate information may be used to make a decision about the individual. (Refer to Data Quality policy 1.40.016).

An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. (Refer to Patient Requests for Correction to

Medical Record policy 1.40.010). If a challenge is not resolved to the satisfaction of the individual, UHN will record the substance of the unresolved challenge in the form of a letter from the patient, to be stored in the patient's medical record. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

Ensuring Safeguards for Personal Health Information

UHN will protect the safety and respect the confidentiality of PHI through appropriate safeguards, as per Information Security & Appropriate Use of Technology policy 1.40.012)

Loss of Personal Health Information

In compliance with PHIPA, UHN will inform patients of the loss, theft or inappropriate access of their PHI as soon as reasonably possible. (See Incident Reporting & Review policy 3.20.005.)

Employee Training & Awareness

UHN will make its employees aware of the importance of maintaining the confidentiality of personal health information. As a condition of employment, all new UHN employees/ agents must sign a Confidentiality Agreement (form D-3236). (See UHN's Code of Workplace Ethics.) All existing UHN employees will be required to re-sign the Confidentiality Agreement **annually**. This safeguard may also be facilitated though contractual provisions.

Ongoing education efforts will be delivered to ensure employees, agents, and third parties are provided with tools, training and support as appropriate to enable them to fulfill their duties as it relates to the privacy of PHI.

UHN is also committed to protecting the privacy of its employees. Employee personal information will only be collected, used, and disclosed as per Personal Information Protection policy 2.10.013.

Exceptions

Any exceptions to this policy must be approved in advance by the director of Privacy and Access and may require the involvement of other groups. The Enterprise Privacy and Access Office may be contacted to initiate the request, by phone at 416-340-4800 ext. 6937 (14-6937) or by email to privacy@uhn.on.ca.

Any exceptions to related policies must be approved in advance by their respective owners.

Enforcement

The Enterprise Privacy and Access Office will monitor adherence to this policy using a risk-based model, and report to the appropriate governance bodies.

Accountability for UHN's compliance with this policy rests with the President and Chief Executive Officer, although other individuals within UHN, authorized agents, and/or third-parties will be responsible for the day-to-day collection and processing of personal health information. In addition, other individuals within UHN are delegated to act on behalf of the Chief Executive Officer, such as the Senior Vice-president and Chief Information Officer or the designated privacy contact person, the director of Privacy and Access.

Breaches of this policy and related privacy policies may be subject to disciplinary action, as outlined in Sanctions for Breaches of Personal Health Information policy 2.50.008 and the Confidentiality Agreement (form D-3236).

UHN and its agents are also subject to the fines and penalties set out in PHIPA.

Responsibilities

Enterprise Privacy and Access Office (EPAO) / Information Security Office (ISO)

- enterprise governance, framework, strategy
- development of enterprise policies, procedures, controls, standards
- reporting and escalation to senior management team/board

Affiliates of UHN

Affiliates of UHN include, but are not limited to:

- foundations
- Global Centre for eHealth
- Techna
- Altum Health
- International Patient Program

Affiliate responsibilities include:

- customizing policies for their own line of business
- implementing their own procedures

Management / Supervisor

- comprehend and adhere to this policy
- develop operating procedures/practices within department (including supporting

documentation that support this policy)
- know where the policies/supporting tips are published on the intranet
- ensure staff, consultants, contractors, fellows, students, vendors and volunteers are knowledgeable of policies, standards and procedures
- ensure that EPAO and ISO are aware of all technologies that are being utilized for storing and transporting PHI and corporate confidential information (CCI)

Physician Offices / Surgeon Offices

- comprehend and adhere to this policy
- develop operating procedures/practices within department (including supporting documentation)
- know where the policies/supporting tips are published on the intranet
- ensure staff are knowledgeable of policies
- ensure that EPAO and ISO are aware of all technologies that are being utilized for storing and transporting PHI and CCI

Employees, Consultants, Contractors, Fellows, Students, Vendors, Volunteers, & Residents

- comprehend and adhere to this policy and supporting departmental procedures
- know where the policies/supporting tips are published on the intranet
- only use technologies that are supported by UHN policies
- ask questions when unsure of a policy or procedure

Related Documents

- Access to Archival Records policy 1.30.008
- Acting with Integrity: A Code of Workplace Ethics
- Confidentiality Agreement (form D-3236)
- Consent for the Collection, Use & Disclosure of Personal Health Information
- Data Ownership, Stewardship & Security of Health Information policy 40.50.004
- Data Quality policy 1.40.016
- Incident Reporting & Review policy 3.20.005
- Information Security & Appropriate Use of Technology policy 1.40.012
- Limiting Collection, Use and Disclosure of Personal Health Information
- Patient Access to the Medical Record policy 1.40.003
- Patient Requests for Correction to Medical Record policy 1.40.010
- Personal Information Protection policy 2.10.013
- Release of Patient Information policy 1.40.002
- Sanctions for Breaches of Personal Health Information policy 2.50.008
- Storage, Transport & Destruction of Confidential Information policy 1.40.006

Definitions

Agent: A person that, with the authorization of UHN, acts for or on behalf of the organization in respect of personal health information for the purposes of UHN and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by UHN and whether or not the agent is being remunerated. Examples of agents of UHN include, but are not limited to, employees, volunteers, students, physicians, residents, fellows, consultants, researchers, vendors.

Confidential information: Confidential information maintained at UHN can fall under three categories, Personal Health Information, Personal Information, and Corporate Confidential Information.

Corporate confidential information (CCI): Information maintained by UHN that is not routinely made publicly available, including financial, administrative, commercial and technical information, and can also include records containing legal advice and employee-related information. These records may be subject to the Freedom of Information and Protection of Privacy Act (FIPPA).

Health information custodian: Listed persons or organizations under the Personal Health Information Protection Act, such as hospitals, who have custody or control of personal health information as a result of the work they do. As a public hospital, UHN is considered to be a health information custodian (as per Personal Health Information Protection Act, 2004, Schedule A, Explanatory Note).

Personal health information (PHI): Any identifying information about an individual relating to the individual's health or to the provision of health care to the individual. For example, an individual's health number and/or medical record would be considered personal health information, subject to the Personal Health Information Protection Act (PHIPA).

Personal information (PI): Identifying information about an individual that does not contain health care information. Examples include an individual's age, religion, address and telephone number. Records that contain PI may be subject to the Freedom of Information and Protection of Privacy Act (FIPPA).

Record of personal health information: The Personal Health Information Protection Act defines a record as personal health information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise.

References

1. ISO/IEC 29100:2011

2. Personal Health Information Protection Act, 2004

3. Personal Information & Protection of Electronic Documents Act, 2004